UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

NAGRAVISION SA,	§	Civil Action No. 4:15-cv-00403
	§	
Plaintiff,	§	
	§	
vs.	§	
	§	
ZHUHAI GOTECH INTELLIGENT TECHNOLOGY CO. LTD; GOTECH INTERNATIONAL TECHNOLOGY LTD.; GLOBALSAT INTERNATIONAL TECHNOLOGY LTD.; and DOES 1-12,	§	
	§	
Defendants.	§	

PLAINTIFF NAGRAVISION'S AMENDED COMPLAINT

1. Plaintiff Nagravision SA ("Nagravision") brings this action against Defendants Zhuhai Gotech Intelligent Technology Co. Ltd., Gotech International Technology Ltd., and Globalsat International Technology Ltd. (collectively, "Defendants") based on their operation of a network of computer servers that illegally capture and rebroadcast Nagravision's control words or "keys" to end users that have purchased Defendants' unauthorized receivers, thereby enabling the end users to circumvent Nagravision's security technology and watch copyrighted television programming provided by Nagravision's customers without paying the required subscription fee.

PARTIES

2. Plaintiff Nagravision SA is a Switzerland corporation with its principal place of business located at 22-24, Route de Genève, 1033 Cheseaux, Switzerland.

3. Defendant Zhuhai Gotech Intelligent Technology Co. Ltd. ("Zhuhai Gotech") is a Hong Kong limited liability company with its principal place of business located at 66 Yongda Road, Hongqi Town, Jinwan District, Zhuhai City, China. Zhuhai Gotech was formerly known as Zhuhai Gotech Electronic Technology Co. Ltd., the name change occurring on or about June

10, 2014. Miao Keliang ("Miao") is believed to have served as chairman, general manager, and the majority shareholder of Zhuhai Gotech. Zhuhai Gotech claims to have subsidiaries located in Hong Kong, Chengdu, Jinggangshan, Shenzhen and Dubai, along with testing centers located in Germany, South Africa, Brazil and France.

4. Defendant Gotech International Technology Ltd. ("Gotech Int'l") is a Hong Kong corporation with its principal place of business located at Room 2506 25F, Prosperity Place, 6 Shing Yip Street, Kwun Tong, Kowloon, Hong Kong. On information and belief, Gotech Int'l is wholly owned by Zhuhai Gotech, and Miao is the sole director of the Gotech Int'l.

5. Defendant Globalsat International Technology Ltd. ("Globalsat") is a Hong Kong corporation with its principal place of business also located at Room 2506 25F, Prosperity Place, 6 Shing Yip Street, Kwun Tong, Kowloon, Hong Kong. On information and belief, Globalsat is wholly owned by a Hong Kong corporation called Globalsat (H.K.) Holdings Ltd., which in turn is wholly owned by Globalsat International Holdings Ltd., a company that is organized under the laws of the British Virgin Islands. Miao Keliang is believed to be the sole owner of Globalsat International Holdings Ltd., and has served as the director and general manager of Globalsat.

6. On information and belief, Defendants Gotech Int'l and Globalsat are subsidiaries which serve as agents for Zhuhai Gotech, the parent company and alter ego of Gotech Int'l and Globalsat. Zhuhai Gotech is believed to authorize, control, participate in, and receive financial benefits from the illicit activities of Gotech Int'l and Globalsat alleged herein. Gotech Int'l and Globalsat are believed to act as agents for and participate in the unlawful activities of each other.

7. Defendants have been operating from shared locations in Hong Kong and China. Globalsat and Gotech Int'l share the same office space in Hong Kong, and Globalsat and Zhuhai Gotech manufacture receivers from the same factory in China, the addresses of which are listed above. Globalsat also conducted business from 17/F and 13/F, China Youse Building, No. 6013, Shennan Avenue, Futian District, Shenzhen, China. The 13/F location is occupied by Shenzhen Starvideocom Technology Co. Ltd., d/b/a Shenzhen MKTech Electronic Technology Co. Ltd.

The foregoing are believed to be additional subsidiaries that are under the control of and which serve as agents for Zhuhai Gotech.

8. Defendant Does 1-12 are individuals or entities that authorize, control, participate in, and receive financial benefits from the illicit activities attributed to Zhuhai Gotech, Gotech Int'l, and Globalsat as alleged herein. Defendant Does 1-12 also include individuals or entities in control of additional servers used in the piracy network set forth below. Nagravision believes that discovery will lead to the identification of Defendant Does 1-12, and allow Nagravision to amend the complaint to list them by name.

JURISDICTION AND VENUE

9. Nagravision is claiming violations of the Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(2) ("DMCA"), and Federal Communications Act, 47 U.S.C. §§ 605(a), (e)(4). ("FCA"). Subject matter jurisdiction is proper in this Court under 28 U.S.C. §§ 1331 and 1338.

10. Upon information and belief, this Court has personal jurisdiction over Defendants under Rule 4(k)(2) of the Federal Rules of Civil Procedure. Defendants use a network of servers located in various cities across in the United States to engage in the unauthorized distribution of Nagravision's control words in violation of the DMCA and FCA. In addition, Defendants import their unauthorized receivers to distributors in the United States, after which the products are sold to end users throughout the United States. Exercising jurisdiction over Defendants is consistent with the Constitution and laws of the United States.

11. Venue is proper in this Court under 28 U.S.C. § 1391(c)(3) because Defendants are nonresidents that may be sued in any judicial district. Venue is also appropriate in this Court under 28 U.S.C. § 1391(b)(3) because Defendants are subject to the personal jurisdiction of this district, and 28 U.S.C. § 1400(a) because Nagravision asserts claims relating to the protection of copyrighted works.

NAGRAVISION'S SECURITY TECHNOLOGY

12. Nagravision is part of the Kudelski Group, a world leader in digital security and convergent media solutions for the delivery of digital and interactive content. Several prominent

broadcasters in the pay-television industry are equipped with Nagravision's technology, which ensures secure access to their subscription-based television services. Nagravision's customers serve markets globally, including DISH Network in the United States, Bell TV in Canada, and other major pay-television broadcasters in North America, South America, Europe, and Asia.

13. Pay-television broadcasters that implement the Nagravision security technology transmit their signal to subscribers in encrypted form. In order to receive the signal, subscribers are required to purchase or lease from the broadcaster a receiver paired with a smart card and a programming subscription package. Viewing rights vary based on the services the subscriber has purchased from the pay-television broadcaster.

14. Nagravision designs and licenses software that is incorporated into the receivers and smart cards, and also manufactures smart cards. The smart card is used to (i) manage, store, and communicate to the receiver the subscriber's right to decrypt specific channels based on his subscription plan, and (ii) decrypt the encrypted control words or "keys" required to unlock and view the channels for which the subscriber has purchased access.

15. Nagravision's control words are transmitted to subscribers in the encrypted audio and video streams of the pay-television broadcaster. The control words are channel specific and change automatically about every five to ten seconds for each channel. Control words are double protected by being delivered in encrypted packets known as "entitlement control messages" or "ECMs". The keys used to decrypt ECMs, called "transmission keys", are stored in the memory of the subscriber's smart card and may be changed by the broadcaster over the air as needed.

16. When a subscriber wants to view a specific pay-television channel, the receiver obtains the ECM containing the encrypted control word and forwards it to the smart card. The smart card uses its current transmission key to decrypt the ECM. The smart card then looks in its rights database to confirm the subscriber purchased a subscription to view the programming the control word will decrypt. If the rights match, the smart card forwards the unencrypted control word to the receiver, where the control word decrypts the broadcast.

17. "Internet key sharing" or "IKS" is a form of pay-television piracy that involves unauthorized harvesting and distribution of Nagravision's control words. Nagravision's control words are obtained by purchasing a subscription with the pay-television broadcaster, and then using a genuine smart card activated on that subscription to decrypt ECMs containing the control words. Once decrypted, control words are sent from the smart card to a computer server, called an "IKS server", where they are saved in the server's memory or cache.

18. Nagravision control words are distributed from the IKS server to end users. End users access the IKS server with an unauthorized receiver connected to the Internet. When the end user tunes to a pay-television channel, the unauthorized receiver requests the control word for that particular channel from the IKS server. The IKS server sends the control word back over the Internet to the unauthorized receiver, enabling the end user to decrypt the channel without having authorization from and without making payment to the pay-television broadcaster.

DEFENDANTS' WRONGFUL CONDUCT

19. Defendant Zhuhai Gotech, according to its website located at *www.gotechcn.com*, "specializes in the provision of digital set-top-boxes" and related products which "are deployed across Europe, the Middle East, Latin America, North Africa and Australia." Zhuhai Gotech's website offers various model receivers and accessories under the MKTech brand.

20. Defendant Globalsat, according to its website located at *www.goosat.com*, "is an aggressive player in the industry [that] suppl[ies] the world with a diverse range of digital set-top-boxes across all television transmission systems including satellite", serving "the markets of Europe, Middle East, Latin America, North Africa and Australia." Globalsat's website offered several model receivers under the Goosat brand.

21. Defendants Zhuhai Gotech, Gotech Int'l, and Globalsat have been operating from the same business locations in China and Hong Kong, including the common production facility. In addition to MKTech and Goosat receivers, Defendants are believed to have manufactured and distributed receivers under the brand names Globalsat, AZAmerica, NAZABox, Captiveworks,

and Limesat, among them the Globalsat GS-111 and GS-300, AZAmerica S1005, NAZABox NZ S-1010, Captiveworks CW-600S, CW-650S, CW-700S, CW-800S, 900 HD, and Limesat Ultra.

22. Globalsat, AZAmerica, and NAZABox receivers are capable of circumventing the Nagravision security system and intercepting the subscription-based television programming that is provided by Nagravision's customers in Latin America, Telefonica and Claro TV Brazil. As stated on Defendants' websites, Latin America is one of the markets targeted by Defendants.

23. Globalsat, AZAmerica, and NAZABox receivers contain several components that are unnecessary for receiving unencrypted satellite broadcasts, but are essential for decrypting broadcasts protected by the Nagravision security system. The components include proprietary Nagravision code taken from the ROM and EEPROM of a pay-television provider's smart card, decryption keys used in the Nagravision security system, control word sharing protocols, menu options to manually enter Nagravision's keys or alternatively configure the receiver to engage in control word sharing via Internet or satellite, and other design elements relating to pay-television piracy.

24. On information and belief, Defendants operate a network of IKS servers that are used to distribute Nagravision's control words to Globalsat, AZAmerica, and NAZBox receivers, among other products. The servers involved are: (i) "authentication servers", which confirm the end user is permitted to access the IKS service and provide information to connect to additional servers that deliver Nagravision's control words; and (ii) "control word servers", which function as a cache by storing Nagravision's control words and also a front end by transmitting the control words from the cache to end users that request the control words through their receiver.

25. On information and belief, the control word servers receive Nagravision's control words from additional servers that have been connected to smart cards activated on subscription accounts held with pay-television providers using Nagravision security technology. The servers are believed to be running control word sharing software that allows them to extract Nagravision control words from the smart cards.

26. The following chart has a non-exclusive list of the IP addresses of authentication servers and control word servers located in the United States which Defendants are believed to operate, and the Globalsat, AZAmerica, and NAZABox receivers supported by those servers.

Server IP Address	Server Type - Reference Name	Unauthorized Receiver(s) Supported By Server
107.167.18.150	Authentication Server 1	AZAmerica S1001, S1001+, S1005, S922; Globalsat GS-111, GS-300; NAZABox NZ S-1010
198.148.86.235	Authentication Server 2	AZAmerica S1001, S1001+, S1005, S922; Globalsat GS-111, GS-300; NAZABox NZ S-1010
23.29.77.220	Authentication Server 3	AZAmerica S1001, S1001+, S1005; Globalsat GS-111, GS-300; NAZABox NZ S-1010
107.167.25.110	Authentication Server 4	AZAmerica S926
107.181.160.16	Authentication Server 5	NAZABox NZ S-1010
208.98.46.110	Authentication Server 6	NAZABox NZ S-1010
107.181.170.31	Control Word Server 7	AZAmerica S922
199.115.96.93	Control Word Server 8	AZAmerica S1001
69.4.231.45	Control Word Server 9	AZAmerica S1005
107.167.12.251	Control Word Server 10	AZAmerica S1005
174.128.234.151	Control Word Server 11	AZAmerica S1005
107.181.160.16	Control Word Server 12	AZAmerica S1001+
199.115.96.91[1]	Control Word Server 13	Globalsat GS-111, GS-300; NAZABox NZ S-1010

27. The IP addresses of several of the foregoing authentication servers, known control word sharing servers, and additional servers that were identified as part of the IKS network and

[1]The IP addresses of additional servers used in the IKS network are assigned to ISPs in Germany, France, and Brazil, where Defendant Zhuhai Gotech claims to maintain its testing centers. There are also other servers in the United States that are part of the IKS network, and thus believed to be operated by Defendants, that Nagravision is continuing to analyze.

servers assigned to Defendants are hardcoded in the factory-installed firmware of the Globalsat, AZAmerica, and NAZABox receivers.

28. Defendants also imported and sold Limesat and Captiveworks brand receivers to distributorships located in the United States. Limesat and Captiveworks receivers are capable of circumventing Nagravision's security system and intercepting the subscription-based television programming that is provided by Nagravision's customer in the United States, DISH Network.

29. Limesat receivers contain several components that are unnecessary for receiving unencrypted satellite broadcasts, but are essential for decrypting broadcasts protected by the Nagravision security system. The components include a decryption algorithm used as part of the Nagravision security system, a LAN port for connecting to an IKS server, smart card reader, and an authentication system that allows the receiver to run infringing software.

30. Captiveworks receivers also contain several components that are characteristic of Nagravision piracy and have no legitimate purpose in the receivers. The components include a decryption algorithm and keys that are used in the Nagravision security system, and proprietary Nagravision code taken from the ROM and EEPROM of a pay-television provider's smart card.

CLAIMS FOR RELIEF

COUNT I

Trafficking in Circumvention Technology, Services, and Products in Violation of the Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(2)

31. Nagravision repeats and realleges the allegations in paragraphs 1-30.

32. On information and belief, Defendants have offered to the public, provided, and otherwise trafficked in control word sharing technology and services in violation of 17 U.S.C. § 1201(a)(2), including by the operation of Authentication Servers 1-6 and Control Word Servers 7-13. Defendants also manufactured, imported, offered to the public, provided, and otherwise trafficked in Limesat and Captiveworks receivers in violation of 17 U.S.C. § 1201(a)(2).

33. Defendants' control word sharing technology, services, and unauthorized receivers are primarily designed and produced to circumvent the Nagravision security system; have no

commercially significant purpose or use other than to circumvent Nagravision's security system; and, upon information and belief, are marketed by Defendants and others known to be acting in concert with them for use in circumventing Nagravision's security system.

34. The Nagravision security technology effectively controls access to, copying, and distribution of copyrighted works. Defendants' actions that constitute violations of 17 U.S.C. § 1201(a)(2) have been performed without permission, authorization, or consent of Nagravision or, on information and belief, any owner of the copyrighted content broadcast on the pay-television platforms protected by Nagravision's security technology. Nagravision is authorized by the pay-television providers to protect their copyrighted content from unauthorized viewing.

35. Defendants willfully violated 17 U.S.C. § 1201(a)(2) for purposes of commercial advantage and private financial gain. Defendants knew or should have known that their actions are illegal and prohibited.

36. Defendants' violations cause damage to Nagravision in an amount to be proven at trial. Unless restrained and enjoined by the Court, Defendants will continue to violate 17 U.S.C. § 1201(a)(2).

COUNT II

Distributing and Assembling Signal Theft Equipment in Violation of the Federal Communications Act, 47 U.S.C. § 605(e)(4)

37. Nagravision repeats and realleges the allegations in paragraphs 1-30.

38. On information and belief, Defendants have manufactured and distributed control word sharing software and assembled servers to offer Nagravision control word sharing services in violation of 47 U.S.C. § 605(e)(4), including Authentication Servers 1-6 and Control Word Servers 7-13. Defendants also manufactured, assembled, imported, sold, and distributed Limesat and Captiveworks receivers in violation of 47 U.S.C. § 605(e)(4).

39. Defendants' control word sharing software, servers, and unauthorized receivers are primarily of assistance in decrypting, without authorization, direct-to-home satellite broadcasts of television programming protected by Nagravision's security technology. Defendants intended

for their control word sharing software, servers, and unauthorized receivers to be used for this purpose.

40. Defendants willfully violated 47 U.S.C. § 605(e)(4) for purposes of commercial advantage and private financial gain. Defendants knew or should have known that their actions are illegal and prohibited.

41. Defendants' violations cause damage to Nagravision in an amount to be proven at trial. Unless restrained and enjoined by the Court, Defendants will continue to violate 47 U.S.C. § 605(e)(4).

COUNT III

Assisting Others to Receive Satellite Signals Without Authorization in Violation of the Federal Communications Act, 47 U.S.C. § 605(a)

42. Nagravision repeats and realleges the allegations in paragraphs 1-30.

43. On information and belief, Defendant have assisted others to receive Nagravision control words and satellite broadcasts of television programming protected by the Nagravision security technology, without authorization and for their own benefit, in violation of 47 U.S.C. § 605(a), including by their operation of Authentication Servers 1-6 and Control Word Servers 7-13. Defendants also assisted others to receive Nagravision control words and satellite broadcasts of television programming protected by the Nagravision security technology by manufacturing, importing, and distributing Limesat and Captiveworks receivers.

44. Defendants willfully violated 47 U.S.C. § 605(a) for the purpose of commercial advantage and private financial gain. Defendants knew or should have known that their actions are illegal and prohibited.

45. Defendants' violations cause damage to Nagravision in an amount to be proven at trial. Unless restrained and enjoined by the Court, Defendants will continue to violate 47 U.S.C. § 605(a).

PRAYER FOR RELIEF

WHEREFORE, Nagravision seeks judgment against Defendants as follows:

A. For a grant of permanent injunctive relief restraining and enjoining Defendants, and any of their officers, agents, servants, employees, attorneys, or other persons acting in active concert or participation with any of the foregoing that receives actual notice of the order, from:

(1) manufacturing, importing, offering to the public, providing, or otherwise trafficking in Nagravision control word sharing technology or services, unauthorized receivers, or any other service, technology, product, device, component, or part thereof that:

(a) is primarily designed or produced for circumventing Nagravision's security system or any other technological measure deployed by Nagravision that controls access to, copying, or distribution of copyrighted works;

(b) has only a limited commercially significant purpose or use other than to circumvent Nagravision's security system or any other technological measure deployed by Nagravision that controls access to, copying, or distribution of copyrighted works;

(c) is marketed for use in circumventing Nagravision's security system or any other technological measure deployed by Nagravision that controls access to, copying, or distribution of copyrighted works;

(2) manufacturing, assembling, modifying, importing, selling, or distributing Nagravision control word sharing software or servers, unauthorized receivers or any other device or equipment knowing or having reason to know that such device or equipment is primarily of assistance in the unauthorized decryption of direct-to-home satellite services protected by the Nagravision security technology;

(3) receiving or assisting others in receiving Nagravision's control words or satellite transmissions of television programming protected by Nagravision's security technology without authorization;

B. For an order impounding and authorizing Nagravision to take possession of and destroy all control word sharing software and technologies, unauthorized receivers, and all other products, components, or parts thereof in the custody or control of Defendants that the Court has

reasonable cause to believe are involved in a violation of the Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(2), or Federal Communications Act, 47 U.S.C. §§ 605(a), (e)(4);

C. For an order directing Defendants to preserve and turn over to Nagravision all records in any form, including electronic documents, that evidence, refer, or relate to any control word sharing server technology or service, unauthorized receivers, or customers of these control word sharing services and receivers.

D. Award Nagravision the greater of its actual damages together with any profits made by Defendants that are attributable to the violations alleged herein, or statutory damages in the amount of up to $2,500 for each violation of 17 U.S.C. § 1201(a)(2), under 17 U.S.C. §§ 1203(c)(2) and 1203(c)(3)(A);

E. Award Nagravision the greater of its actual damages together with any profits made by Defendant that are attributable to the violations alleged herein, or statutory damages in the amount of up to $100,000 for each violation of 47 U.S.C. § 605(e)(4), under 47 U.S.C. § 605(e)(3)(C)(i);

F. Award Nagravision the greater of its actual damages together with any profits made by Defendants that are attributable to the violations alleged herein, or statutory damages in the amount of up to $10,000 for each violation of 47 U.S.C. § 605(a), pursuant to 47 U.S.C. § 605(e)(3)(C)(i). Nagravision seeks to increase that amount by $100,000 for each violation, at the Court's discretion, in accordance with 47 U.S.C. § 605(e)(3)(C)(ii);

G. Award Nagravision its costs, attorney's fees, and investigative expenses under 17 U.S.C. § 1203(b)(4)-(5) and 47 U.S.C. § 605(e)(3)(B)(iii);

H. For a full and accurate accounting of all profits and other benefits received by Defendants as a result of the wrongful conduct described herein;

I. For pre and post-judgment interest on all damages awarded, from the earliest date permitted by law at the maximum rate permitted by law;

J. For such additional relief as the Court deems just and equitable.

Dated: August 6, 2015.

Respectfully submitted,

HAGAN NOLL & BOYLE, LLC

s/ Chad M. Hagan
Chad M. Hagan (attorney-in-charge)
Texas Bar #24036700
S.D. Tex. Bar #36439
Two Memorial City Plaza
820 Gessner, Suite 940
Houston, Texas 77024
Telephone: (713) 343-0478
Facsimile: (713) 758-0146
chad.hagan@hnbllc.com

Timothy M. Frank (of counsel)
Texas Bar #24050624
S.D. Tex. Bar #614705
timothy.frank@hnbllc.com

Attorneys for Plaintiff Nagravision SA